

**Notice of Allowability**

Application No.

10/692,493

Examiner

Chuong D. Ngo

Applicant(s)

SUGA, YUJI

Art Unit

2193

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to applicant's response filed on 10/03/2007.
2. ☒ The allowed claim(s) is/are 1-17.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All    b) ☐ Some\*    c) ☐ None    of the:
  1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

/Chuong D Ngo/  
Primary Examiner, AU 2193

### EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's representative, Trevor Chuang, on 10/11/2007.

2. The application has been amended as follows:

In claim 1, line 1, after "for", inserted - - for encrypting or decrypting data by - -; and  
line 18, after "c", changed "as  $x^e$ " to - - for encrypting or decrypting data - -.

In claim 2, line 1, after "for", inserted - -for encrypting or decrypting data by- -; and  
line 18, after "c", changed "as  $x^e(\text{mod}N)$ " to - -for encrypting or decrypting data- -.

In claim 14, line 16, after "c", changed "as  $x^e$ " to - - for encrypting or decrypting data - -.

In claim 15, line 16, after "c", changed "as  $x^e(\text{mod}N)$ " to - - for encrypting or decrypting data - -.

In claim 16, line 2, after "for", inserted - - for encrypting or decrypting data by - -; and  
line 17, after "c", changed "as  $x^e$ " to - - for encrypting or decrypting data - -.

In claim 17, line 2, after "for", inserted - -for encrypting or decrypting data by- -; and  
line 17, after "c", changed "as  $x^e(\text{mod}N)$ " to - -for encrypting or decrypting data- -.

Art Unit: 2193

3. The following is an examiner's statement of reasons for allowance:

The prior art of record does not teach or fairly suggest an exponent calculation apparatus having a combination of elements including a candidate exponents storing unit, a pre-calculation unit, a pre-calculated values storing unit and a dividing unit as recited in claims 1,2 and 14-17.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chuong D. Ngo whose telephone number is (571) 272-3731. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2193

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Chuong D Ngo/  
Primary Examiner  
Art Unit 2193

10/11/2007